PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PU030241	FOR FURTHER ACTION	See Form PCT/IPEA/416
International application No. PCT/US2004/002407	International filing date *(day/month/year)* 27.01.2004	Priority date *(day/month/year)* 13.08.2003
International Patent Classification (IPC) or national classification and IPC H04L29/06		
Applicant THOMSON LICENSING S.A. et al.		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 6 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. ☒ *sent to the applicant and to the International Bureau)* a total of 4 sheets, as follows:
      ☐ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.
   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☒	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

Date of submission of the demand	Date of completion of this report
31.01.2005	07.11.2005
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Bengi-Akyuerek, K Telephone No. +49 89 2399-7105

Form PCT/IPEA/409 (Cover Sheet) (January 2004)

IAP12 Rec'd PCT/PTO 08 FEB 2006

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/US2004/002407

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:
   - ☐ international search (under Rules 12.3 and 23.1(b))
   - ☐ publication of the international application (under Rule 12.4)
   - ☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

Description, Pages	
1-12	as originally filed
Claims, Numbers	
1-28	received on 02.02.2005 with letter of 31.01.2005
Drawings, Sheets	
1/7-7/7	as originally filed

   ☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. ☐ The amendments have resulted in the cancellation of:
   - ☐ the description, pages
   - ☐ the claims, Nos.
   - ☐ the drawings, sheets/figs
   - ☐ the sequence listing *(specify)*:
   - ☐ any table(s) related to sequence listing *(specify)*:

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).
   - ☐ the description, pages
   - ☐ the claims, Nos.
   - ☐ the drawings, sheets/figs
   - ☐ the sequence listing *(specify)*:
   - ☐ any table(s) related to sequence listing *(specify)*:

* *If item 4 applies, some or all of these sheets may be marked "superseded."*

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/US2004/002407

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-28
	No:	Claims	-
Inventive step (IS)	Yes:	Claims	1-28
	No:	Claims	-
Industrial applicability (IA)	Yes:	Claims	1-28
	No:	Claims	-

2. Citations and explanations (Rule 70.7):

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (SEPARATE SHEET)

International application No.
PCT/US2004/002407

Re Item V

Reasoned statement under Article 35(2) PCT with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 The following documents cited in the International Search Report are referred to in this communication:

D1: WO 02/47356 A (DIEHL ERIC; ANDREAUX JEAN PIERRE (FR); CHEVREAU SYLVAIN (FR); THOM) 13 June 2002 (2002-06-13)
D2: WO 01/59549 A (KONINKL PHILIPS ELECTRONICS NV) 16 August 2001 (2001-08-16)

2 The present invention relates to an apparatus (**claim 1**) and methods (**claims 10 and 16**) for secure content delivery over communication networks.

3 The subject-matter of the present application appears to be novel and inventive over the cited prior art (Article 33(2) and (3) PCT) and therefore meets the criteria mentioned in Article 33(1) PCT:

3.1 Document **D1**, which is considered as closest prior art, discloses with regard to the broadest **claim 1**:

A device ("receiver"; Fig. 1, ref. 2), located at a remote site in communication with a network having one server ("source"; Fig. 1, ref. 1) comprising means for:
(a) receiving a first information item comprising an access code ("secret identifier"; Fig. 1, ref. I5) and a content key ("control word"; Fig. 1, ref. CW) scrambled by using an [encryption] key ("SSK") known by the remote site (page 5, line 37 to page 6, line 2: "...the encrypted control word...and the secret identifier...are encrypted with this session key SSK at the level of the source 1 before being transmitted to the receiver...");
(b) descrambling the first information item by using a corresponding decrypting key (page 6, lines 1-2: "...the receiver 2 which decrypts them with the aid of the same session key SSK");
(c) receiving a second information item ("scrambled data"; Fig. 1, ref. 3),

scrambled by using the content key before the server has verified the access code (page 5, lines 4-5: "the content is transmitted from the source 1 to the receiver 2 in the form of scrambled data 3 scrambled by a control word...").

3.2 As a result, the main difference between the subject-matter of **claim 1** and that of document **D1** resides in that the method also comprises the step of transmitting and verifying the access code, being generated in response to a request for the second information item by a content requester, before delivering the requested content to the claimed device.

3.3 Therefore, the objective problem underlying **claim 1** is regarded as how to enable secure content delivery to a content consumer when content consumer and content requester represent different hosts.

3.4 In view of the teachings of document **D1**, the person skilled in the art would not arrive at the proposed solution to the above-mentioned problem since **D1**, although dealing with secure content delivery between content source and receiver, neither includes a hint to the problem of coping with different content consumer and content requester hosts nor suggests the requester-initiated generation and server-based verification of a transmitted access code before allowing content delivery to a content consumer. Rather, **D1** teaches content transfer by means of a secret identifier used for source authentication before the required encryption keys are transmitted by the content source to the content receiver while being silent as to the request-based generation and transmission of an access code for verification purposes.

3.5 Equally, document **D2** neither alone nor in combination with **D1** discloses or suggests the subject-matter of **claim 1** since its teaching is directed to encrypted content delivery from a provider to a consumer before performing authentication thus leading away from verifying a generated access code before secure content transfer.

4 In the light of the above-mentioned reasons regarding apparatus **claim 1**, the subject-matter of independent method **claims 10 and 16** is also considered novel and inventive,

since it is directed to corresponding method steps performed by complementary units.

Re Item VII

Certain defects in the International Application

1 The independent claims are not properly drafted in the two-part form recommended by Rule 6.3(b) PCT and do not include reference signs in parentheses to increase their intelligibility according to Rule 6.2(b) PCT.

2 The most relevant prior art documents are not properly acknowledged in the description part according to Rule 5.1(a)(ii) PCT.

CLAIMS:

1. A device, located at a remote site in communication with a network having at least one server, comprising:

a processor in communication with a memory, said processor operable to execute code for:

receiving a first information item comprising an access code and a content key scrambled using a key known by said remote site, said access code generated in response to a request for a second information item by a content requester;

descrambling said first information item using a corresponding decrypting key;

transmitting said access code to a server hosting said second information item; and

receiving said second information item scrambled using said content key after said server hosting the second information item verifies said access code.

2. The device as recited in claim 1, wherein said processor is further operable to execute code for:

descrambling said second information item using said content key.

3. The device as recited in claim 1, wherein said first information item includes a use-limit indication.

4. The device as recited in claim 1, wherein said processor is further operable to execute code for:

transmitting said unencrypted access code selected from the group consisting of: automatically, at a predetermined time, at a predetermined time offset, responsive to a manual input.

5. The device as recited in claim 1, wherein said content key is selected from the group consisting of: a public key, a shared key.

6. The device as recited in claim 3, wherein said use-limit indication is selected from the group consisting of: number of uses, time-period.

7. The device as recited in claim 1, wherein said first information item further includes a content location.

8. The device as recited in claim 7, wherein said processor is further operable to execute code for transmitting said content location.

9. The device as recited in claim 7, wherein said content location is known.

10. A method, operable at a receiving device located at a remote site in communication with a network having at least one server, for descrambling secure content received over said network, said method comprising the steps of:

receiving a first information item comprising an access code and a content key scrambled using a key known by said remote site, said access code generated in response to a request for a second information item by a content requester;

descrambling said first information item using a corresponding decrypting key;

transmitting said access code to a server hosting said second information item;

receiving said second information item, scrambled using said content key, after the server hosting the second information verifies said access code; and

descrambling said second information item using said content key.

11. The method as recited in claim 10, wherein said first information item includes a use-limit indication.

12. The method as recited in claim 10, wherein said content key is selected from the group consisting of: a public key, a shared key.

13. The method as recited in claim 11, wherein said use-limit indication is selected from the group consisting of: number of uses, time-period.

14. The method as recited in claim 10, wherein said first information item further includes a content location.

15. The method as recited in claim 14, wherein said content location is known.

16. A method for transferring secure content over a network comprising the steps of:

receiving a request for content at a first server over a first network from a file requesting device, said request including an encryption key known to a designated remote site;

generating a first information containing an access code and a content key at said server in response to said request for content by said file requesting device;

transferring said first information item to said designated remote site having a file receiving device, wherein said access code and said content key are scrambled using said encryption key;

receiving said access code from said designated remote site having said file receiving device; and

transferring over a second network said secure content after verification of said access code, wherein said secure content is encrypted using said content key.

17. The method as recited in claim 16, wherein said first network and said second network are the same network.

18. The method as recited in claim 16, wherein said file requesting device is selected from the group consisting of: personal digital assistant, cellular telephone, notebook computer and personal computer.

19. The method as recited in claim 16, wherein said file receiving device is selected from the group consisting of: personal digital assistant, cellular telephone, notebook computer and personal computer.

20. The method as recited in claim 16, wherein said first network is a wireless network.

21. The method as recited in claim 16, wherein said first information item includes a location of said content.

22. The method as recited in claim 16, further comprising the step of:

transmitting said content to at least one other server in communication with said first server, wherein said content is scrambled using said content key.

23. The method as recited in claim 22, further comprising the steps of:

transferring over a second network said secure content after verification of said access code, wherein said secure content is scrambled using said content key.

24. The method as recited in claim 16, wherein the step of transferring said access code and said content key is over said first network.

25. The method as recited in claim 16, wherein the step of transferring said access code and said content key is over said second network.

26. The method as recited in claim 16, wherein said second network is a high-speed network.

27. The method as recited in claim 26, wherein said second network is a content delivery network.

28. The method as recited in claim 16, further comprising the step of:

transferring a location of said content to said designated remote site.